CLAIMS

What is claimed is:

1. A method for detecting abnormal activity of a server application user, the method comprising:

(a) measuring a predetermined activity of a server application user over a first predetermined time for generating a first measurement;

(b) measuring the predetermined activity of the server application user over a second predetermined time for generating a second measurement; and

(c) determining whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the server application user.

2. The method of claim 1, comprising maintaining a log of the predetermined activity of the server application user over the first and second predetermined times.

3. The method of claim 1, wherein the predetermined activity comprises a server application request.

4. The method of claim 3, wherein the server application request is an hypertext transfer protocol (HTTP) request.

5. The method of claim 1, wherein the predetermined activity comprises failed login attempts.

6. The method of claim 1, wherein the predetermined activity comprises login time.

7. The method of claim 1, wherein the predetermined activity comprises web page requests.

8. The method of claim 3, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

9. The method of claim 7, wherein the second measurement is an average count of web page requests for communication sessions between the server application user and a server application.

10. The method of claim 7, wherein the second measurement is an average count of web page requests between the server application user and a server application during a time interval.

11. The method of claim 1, wherein the predetermined activity comprises failed web page requests.

12. The method of claim 11, wherein the second measurement is an average count of failed web page requests for communication sessions between the server application user and a server application.

13. The method of claim 1, wherein the predetermined activity comprises session duration.

14. A system for detecting abnormal activity of a server application user, the system comprising:

(a) a network interface for receiving communication data of a predetermined activity of a server application user over a first and second predetermined time, respectively; and

(b) a detector operable to generate a first and second measurement of the predetermined activity for the first and second

predetermined times, respectively, and operable to determine whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the server application user.

15. The system of claim 14, comprising a log operable to maintain a record of the predetermined activity of the server application user over the first and second predetermined times.

16. The system of claim 14, wherein the predetermined activity comprises a server application request.

17. The system of claim 16, wherein the server application request is an hypertext transfer protocol (HTTP) request.

18. The system of claim 14, wherein the predetermined activity comprises failed login attempts.

19. The system of claim 14, wherein the predetermined activity comprises login time.

20. The system of claim 14, wherein the predetermined activity comprises web page requests.

21. The system of claim 20, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

22. The system of claim 20, wherein the second measurement is an average count of web page requests for communication sessions between the server application user and a server application.

23. The system of claim 20, wherein the second measurement is an average count of web page requests between the server application user and a server application during a time interval.

24. The system of claim 14, wherein the predetermined activity comprises failed web page requests.

25. The system of claim 24, wherein the second measurement is an average count of failed web page requests for communication sessions between the server application user and a server application.

26. The system of claim 14, wherein the predetermined activity comprises session duration.

27. A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) measuring a predetermined activity of a server application user over a first predetermined time for generating a first measurement;

(b) measuring the predetermined activity of the server application user over a second predetermined time for generating a second measurement; and

(c) determining whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the server application user.

28. The computer program product of claim 27, comprising maintaining a log of the predetermined activity of the server application user over the first and second predetermined times.

29. The computer program product of claim 14, wherein the predetermined activity comprises a server application request.

30. The computer program product of claim 29, wherein the server application request is an hypertext transfer protocol (HTTP) request.

31. The computer program product of claim 27, wherein the predetermined activity comprises failed login attempts.

32. The computer program product of claim 27, wherein the predetermined activity comprises login time.

33. The computer program product of claim 27, wherein the predetermined activity comprises web page requests.

34. The computer program product of claim 33, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

35. The computer program product of claim 33, wherein the second measurement is an average count of web page requests for communication sessions between the server application user and a server application.

36. The computer program product of claim 33, wherein the second measurement is an average count of web page requests between the server application user and a server application during a time interval.

37. The computer program product of claim 27, wherein the predetermined activity comprises failed web page requests.

38. The computer program product of claim 37, wherein the second measurement is an average count of failed web page requests for

communication sessions between the server application user and a server application.

39. The computer program product of claim 27, wherein the predetermined activity comprises session duration.

40. A method for detecting abnormal activity of a server application user, the method comprising:

(a) measuring a predetermined activity of a plurality of server application users over a first predetermined time for generating a first measurement;

(b) measuring the predetermined activity of a first server application user over a second predetermined time for generating a second measurement; and

(c) determining whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the first server application user.

41. The method of claim 40, comprising maintaining a log of the predetermined activity over the first and second predetermined times.

42. The method of claim 40, wherein the predetermined activity comprises web page requests.

43. The method of claim 42, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

44. The method of claim 40, wherein the second measurement is average count of web page requests for communication sessions between the server application user and a plurality of server applications.

45. The method of claim 40, wherein the predetermined activity comprises session duration.

46. The method of claim 40, wherein the second measurement is average session duration for communication sessions between the server application user and a plurality of server applications.

47. A system for detecting abnormal activity of a server application user, the system comprising:

(a) a network interface for receiving communication data of a predetermined activity of a first server application user and a selected plurality of server application users over a first and second predetermined time, respectively; and

(b) a detector operable to generate a first and second measurement of the predetermined activity for the first and second predetermined times, respectively, and operable to determine whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the first server application user.

48. The system of claim 47, comprising a log for recording the predetermined activity over the first and second predetermined times.

49. The system of claim 47, wherein the predetermined activity comprises web page requests.

50. The system of claim 49, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

51. The system of claim 49, wherein the second measurement is average count of web page requests for communication sessions between the server application user and a plurality of server applications.

52. The system of claim 47, wherein the predetermined activity comprises session duration.

53. The system of claim 47, wherein the second measurement is average session duration for communication sessions between the server application user and a plurality of server applications.

54. A computer program product comprising computer-executable instructions embodied in a computer-readable medium for performing steps comprising:

(a) measuring a predetermined activity of a plurality of server application users over a first predetermined time for generating a first measurement;

(b) measuring the predetermined activity of a first server application user over a second predetermined time for generating a second measurement; and

(c) determining whether the first and second measurements deviate a predetermined amount to detect abnormal activity for the first server application user.

55. The computer program product of claim 54, comprising maintaining a log of the predetermined activity over the first and second predetermined times.

56. The computer program product of claim 54, wherein the predetermined activity comprises web page requests.

57. The computer program product of claim 56, wherein the web page requests are hypertext transfer protocol (HTTP) requests.

58. The computer program product of claim 54, wherein the second measurement is average count of web page requests for communication sessions between the server application user and a plurality of server applications.

59. The computer program product of claim 54, wherein the predetermined activity comprises session duration.

60. The computer program product of claim 54, wherein the second measurement is average session duration for communication sessions between the server application user and a plurality of server applications.